



Controller's Quarterly

California Economic Challenges

Kathleen Connell, California State Controller

January 1999

Contents:

Controller's Message	2
Economic Outlook	3
Overview of the Year 2000 Challenge	5
Global Impacts of Y2K	7
Business Continuation Planning	9
Local Government Y2K Planning	11
Survey of Y2K Liability Legislation	13
Facts & Figures	15



Message From State Controller **Kathleen Connell**

Few events in history have been heralded with as much fanfare as the pending arrival of the New Millennium. Beyond the excitement, however, there is cause for concern: most of the technology that society now depends on is based on computer programming that cannot interpret dates beyond 1999. This edition of the *Controller's Quarterly* examines the Year 2000 challenge as it impacts California's economy, businesses, and citizens.

The Millennium Bug, as many call it, involves more than just computers. In this electronic age, anything containing a microchip is potentially vulnerable to the effects of the coming date change, from power systems and phone networks, to elevators and ATM machines. It is truly a universal phenomenon, affecting governments at all levels, businesses large and small, organizations and individuals.

Ensuring their systems are Year 2000 compliant should be the top priority for businesses and public agencies; the consequences of inaction range from the mildly inconvenient to potentially life threatening. Unfortunately, much of the work that remains to be done may not be completed in time, as reported by our guest author from a firm that tracks Year 2000 compliance worldwide.

While many enterprises, public and private, will be fully prepared for the change of century, they still could experience major disruptions due to non-compliance by their business partners or other entities on which they depend to conduct business. This could result in litigation costing billions of dollars, with a serious impact on the economy. Potential legislative remedies are discussed by a guest author who surveyed proposed state and federal laws in this area.

Internal readiness issues for small and medium-size businesses, which face different financial and operational issues than larger enterprises, are presented by two authors who stress the importance of business continuation plans. California's local governments also face special challenges, as reported in the article by a county official who co-chairs a statewide task force that surveyed compliance efforts at the local level.

As California's chief financial officer, I am strongly committed to raising awareness of the Year 2000 issue and its significance to our state's economic health. An informed public helps focus government and corporate entities on the importance of preparing their systems and assists in the global effort to ring in the New Millennium on a positive note for everyone.

KATHLEEN CONNELL

Controller
State of California

January 1999

California Economy

Controller's Outlook

The National Outlook

The past year has been a wild ride for the economy. The stock market took a breather in the summer, and there was talk of recession. However, the bear market turned out to be the shortest in history. In the span of one month in the fall, the Federal Reserve cut interest rates by 75 points. It appears this was all the markets and consumers needed to recover their faith in the economy. Since October, the stock market regained its losses from earlier in the year. There are no signs that consumers have pulled back on spending.

Up until a short time ago, the international economy gave indications that the financial turmoil of the past year had calmed. Just as the world was recovering from the collapse of the Russian ruble, concerns were raised that the turbulence might spread to Latin America. Brazil seemed particularly vulnerable; the response of the International Monetary Fund appeared to have stabilized that situation. On January 13, however, Brazil devalued its currency in response to mounting pressures on the real, reigniting uncertainty in financial markets. While most agree that the situation in the developing world continues to be fragile, the U.S. economy to date appears to be weathering the storm. Job growth in the U.S. slowed in 1998, but unemployment remains low and wages outpaced inflation for the year.

The California Outlook

California exports to the Asian/Pacific countries began to

contract in 1997. The trend accelerated in 1998. Over the past year, California experienced export losses to China, Hong Kong, and Australia, countries that in 1997 had partially offset export losses to the rest of Asia. Exports to Mexico, another country that was providing a cushion in 1997, also are slowing. Figure 1 summarizes the California export picture.

This pronounced drop in exports to Asia, along with the slowdown in exports to Mexico in the coming months, is likely to contribute to more moderate job growth in the state. The Controller's Council of Economic Advisors expects employment gains in 1999 will drop to 2.1% (Figure 2). In 1998, California's economy generated roughly 370,000 jobs, according to Employment Development Department (EDD) official employment data, for a gain of 2.8%. Figures 3 and 4 depict California and U.S. job growth

over the past eight quarters.

The Controller's Council anticipates that the moderation in job growth will cause a slight rise in California's unemployment rate, to roughly 6.0% for 1999. This compares to an average unemployment rate of 5.9% in 1998. Personal income growth is projected to slow to 5.2%.

Figure 1

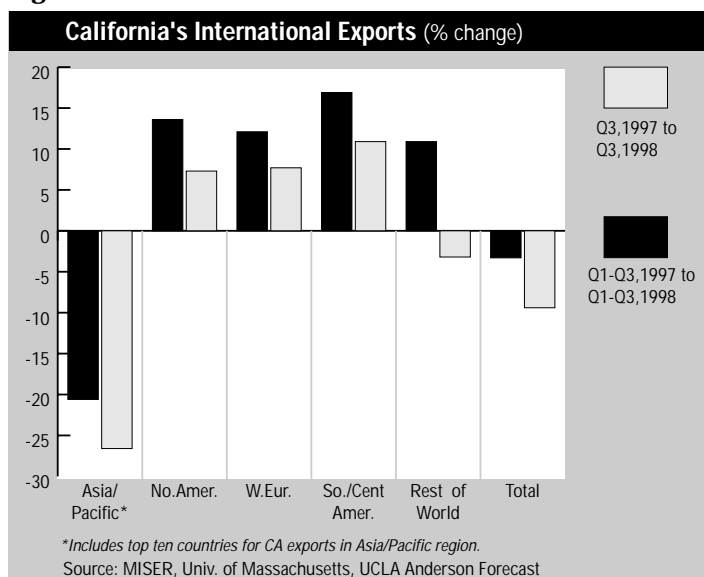


Figure 2

1999 Forecast by Controller's Council of Economic Advisors

Council Member	Employment Growth (Annual %)	Unemployment (Annual %)	Personal Income Growth (Annual %)	Res. Building Permits (Thou)
LA Economic Devt. Corp. (J. Kyser)	2.1%	5.8%	5.6%	125
Calif. Assn. of Realtors (G.U. Krueger)	1.9%	6.1%	4.8%	150
UCLA Anderson Forecast (T. Lieser)	2.4%	6.1%	5.3%	150
UC Berkeley, Center for Real Estate & Urban Economics (C. Kroll)	2.0%	6.0%	5.0%	125
Pacific Bell (J. Hurd)	2.0%	5.8%	5.2%	135
Mean	2.1%	6.0%	5.2%	137
Median	2.0%	6.0%	5.2%	135
State Controller	2.0%	6.0%	5.1%	130
1998 Actual*	2.8%	5.9%	6.6%	125

* "Actual" figures may vary from prior published figures to reflect new data that has become available.

Source: State Controller's Office; Council of Economic Advisors

"This pronounced drop in exports to Asia, along with the slowdown in exports to Mexico in the coming months, is likely to contribute to more moderate job growth in the state."

The housing sector was strong in 1998, with both sales and building permits rising sharply. This stemmed largely from mortgage interest rates remaining low for most of the year. It is estimated that permits for residential construction totaled 125,000 in 1998, a 12.6% increase over 1997. The Controller's Council forecasts residential construction will reach 137,000 units in 1999.

Employment

Construction jobs posted the highest growth rate of any sector of the economy: from November 1997 to November 1998 the annual rate of increase was 9.4%. The next strongest growth occurred in service jobs, which increased by 4.1% in the past year. A new addition to the fast-growth category in 1998 was the finance, insurance, and real estate industry (FIRE). This is related to the strong showing of the real estate industry. Interestingly, the fastest growth in that sector has been employment in non-depository institutions, including consumer fi-

nance and mortgage institutions. The California Association of Realtors reported in its 1998 housing survey that mortgage bankers issued 61.6% of all new mortgages issued in California in 1998, the highest proportion since the survey began in 1981. Savings and loan institutions issued only 20.2% of new mortgages in 1998.

Real Estate

In the fourth quarter of 1998, the median price of a home in California finally reached the peak achieved in the first quarter of 1991. In the first ten months of 1998, sales were 13.8% higher than during the same period of 1997. Prices in Los Angeles began a substantial recovery. In October 1998, the median sale price of a home in the county rose 8.1% over the previous October.

Although sales statewide slowed somewhat recently, the supply of homes on the market is the lowest since 1988. The price discount (less than 2%) and median time on the market (four weeks) are also the

lowest since 1988. In this tight housing market, with interest rates expected to stay low throughout 1999, further price appreciation is likely.

Residential Construction

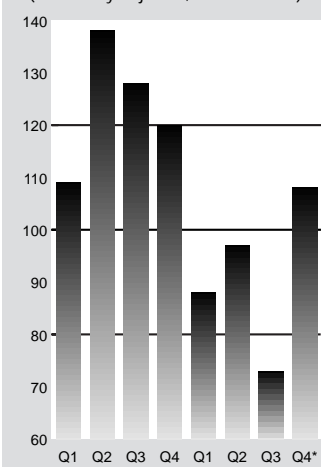
The Sacramento metropolitan region experienced the largest increase in construction. Building permits were up almost 45% in the three-county region that includes Sacramento, Placer, and El Dorado counties. The San Francisco Bay region (with the exception of Alameda and Santa Clara counties) and the San Joaquin Valley also experienced strong rates of increase. San Francisco, one of nine counties that comprise the Bay region, saw a 78% increase in residential construction. The value of non-residential construction permits grew by 20.8% in the first ten months of 1998, with Southern California showing the greatest increase, 35%. In the Bay Area, the rate was 3.7%.

Personal Income

Personal income growth in California remained strong in 1998, estimated at 6.6% by the UCLA Anderson Forecast. (It should be noted that the Commerce Department has revised the components of personal income, which makes comparisons with earlier years somewhat difficult.) This is expected to slow in 1999, primarily due to the employment picture. However, turbulence in the stock market also may contribute to the lower growth rate. Income tax receipts in the last quarter indicate the slowing may already have begun.

Figure 3

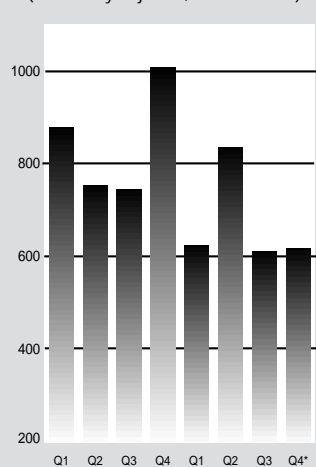
California Non-Farm Payroll Growth
(Seasonally Adjusted, In Thousands)



Source: Employment Development Dept. *Estimate

Figure 4

U.S. Non-Farm Payroll Growth
(Seasonally Adjusted, In Thousands)



Source: U.S. Bureau of Labor Statistics *Estimate

The New Millennium Meeting the Technology Challenge of the Year 2000

Known variously as the Millennium Bug, the Y2K challenge, or simply the biggest computer headache of the century, the coming change of date associated with the Year 2000 poses a challenge of unknown proportions. Around the globe, corporations and governments, individuals and small businesses all face the daunting task of preparing not only computers but virtually any device containing a microchip for the new set of dates. (Figure 1 depicts Year 2000 compliance by industrial sector.)

This overview explores the following key questions that need to be addressed before the New Millennium arrives:

1) How can policy makers clarify the otherwise murky issue of liability that arises when the best efforts of an organization to be Year 2000 compliant are undone by the non-compliance of an external entity on which it depends to conduct its business?

2) Is the average citizen adequately informed on Year 2000 issues? Can expanded public dialogue on the subject raise the level of accountability and compliance by public and private institutions?

The State Controller's Office and the Year 2000

Preparing for the change of century is particularly vital at the State Controller's Office. It plays a central role in the business affairs of the State; any interruption in its core functions

would severely impact the State of California's ability to meet its obligations to citizens, vendors, government agencies, and employees. These functions include auditing and issuing payments to the State's vendors, issuing benefit payments to recipients of aid programs, collecting overdue taxes due the State, managing the State's personnel and payroll system, monitoring the State's cash flow, and reporting on the State's fiscal condition.

Given its importance to the overall business affairs of state government, the Controller's Office has taken steps to ensure its systems are Year 2000 compliant. Following guidelines issued by the Department of Information Technology — the agency with overall responsibility for the State of California's Y2K compliance —

the Controller's Office has inventoried its technology assets, assessed its exposure to the Millennium bug, developed strategies to address Y2K issues and, as of the close of 1998, remediated all of its mission-critical systems. Throughout 1999, the Controller's Office will continue to test its readiness and assist business partners in their Y2K preparations.

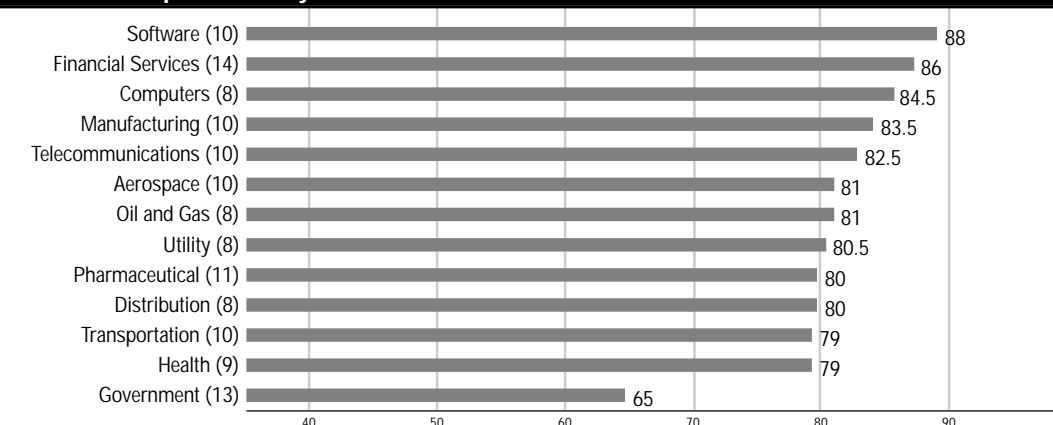
Significance of External Compliance Issues

Year 2000 preparedness goes beyond the efforts of individual organizations. External interfaces, those multiple entities an enterprise relies on to conduct its business, also determine whether an enterprise will be able to conduct business as usual after December 31, 1999. Indeed, in this age of interconnected systems and

"Given its importance to the overall business affairs of state government, the Controller's Office has taken steps to ensure its systems are Year 2000 compliant."

Figure 1

Year 2000 Preparedness By Sector



Rankings based on combination of project progress and risk failure factors for each sector. Number in parentheses represents the number of survey respondents in the category.

Source: Cap Gemini America, October 1998

"An organization that has invested the time and resources to ensure its internal readiness for the Year 2000, yet is unable to deliver goods or services after December 31, 1999, due to an external interface, may be exposed to liability for its failure to deliver...By responding sooner rather than later, policy makers have an opportunity to prevent a bad situation from becoming worse."

networks, "Beware the Weak Link" should be the cautionary motto of Y2K planners.

This issue can be illustrated by the Controller's Office, whose Year 2000 project is typical of what many large enterprises have done to prepare their systems. Like these other enterprises, the Controller's Office must be concerned with its external interfaces. For instance, many of its payments are issued electronically. This involves interfaces with banks that hold the accounts and phone systems that transmit the payment data. If these entities are not Y2K compliant, or encounter their own disruptions due to problems with *their* external interfaces, the ability of the Controller's Office to conduct business in the manner its customers require will be severely undermined. Like any enterprise, operations of the Controller's Office also require the basic infrastructure — electrical power, communications, transportation, to name a few — to continue

working without disruption.

Failures caused by the non-compliance of external interfaces raise troubling liability questions. An organization that has invested the time and resources to ensure its internal readiness for the Year 2000, yet is unable to deliver goods or services after December 31, 1999, due to an external interface, may be exposed to liability for its failure to deliver. This is an area of uncertainty that may require legislative intervention *before* such events occur. By responding sooner rather than later, policy makers have an opportunity to prevent a bad situation from becoming worse.

Public Awareness of Y2K

A critical component of Year 2000 planning is raising public awareness of the issue and disruptions that may be in store. Individuals who have computers in their home are not the only ones affected. Potential impacts on consumers include power outages, loss of phone

service, difficulty in paying bills with credit cards or even checks, loss of official records, and slowdowns in a variety of public services. At the global level, some economists predict disruptions of economic activity that could lead to a recession.

As public awareness increases, the level of compliance in both the public and private sector is likely to rise along with it. Informed citizens will demand assurances from providers of goods and services that they have taken the necessary steps to maintain normal business operations; they will hold these providers accountable if there are disruptions. (Figure 2 reflects the latest survey findings regarding Americans' awareness and expectations of Year 2000 compliance.)

While the New Millennium brings with it uncertainty about the readiness of the world's technology systems, one fact is indisputable: the deadline is immovable and it affects everyone.

Figure 2

Americans and the Y2K Millennium Computer Bug (percentage of respondents to survey conducted Dec. 9-13, 1998)				
Seen or heard about Y2K issue:	A great deal 39%	Some 40%	Not much 13%	Nothing 8%
Believe Y2K computer issue will cause:	Major problems 34%	Minor problems 51%	No problems at all 10%	No opinion 5%
Level of concern about Y2K issue:	Very concerned 16%	Somewhat concerned 40%	Not too concerned 31%	Not at all concerned 13%
Likelihood that banking and accounting systems will fail, possibly causing errors in paychecks, government payments, and other automated financial transactions:		Likely 63%	Unlikely 36%	No opinion 1%
Likelihood that city or county emergency "911" communications systems will fail, putting citizens at risk:		Likely 36%	Unlikely 62%	No opinion 2%
Level of confidence that following entities will upgrade their computer systems before Y2K problems occur:		Confident	Not confident	No opinion
U.S. government		68%	29%	3%
Respondent's state government		73%	25%	2%
Respondent's local government		68%	30%	2%
US corporations and large businesses		82%	16%	2%
US small businesses		56%	41%	3%

Source: Gallup Organization (survey of 1,032 adults nationwide; margin of error is plus or minus 3%)

The View of Year 2000 from 1999



By Dale Vecchio
*Research Director
Gartner Group*

As we enter 1999, the "Year 2000 problem" has changed from simply a computer problem to one that impacts all areas of an organization. In addition to greater focus on other technology areas such as desktop and embedded systems, organizations also are spending a significant portion of their effort on the non-IT aspects of this problem. According to Gartner research, companies are now spending as much time and money on Year 2000 issues outside of IT as they are on the more traditional technology areas associated with the problem.

While continuing their battle with the bug, many companies are now looking at the impact of supply chain failures on their business. In fact, many companies that have never constructed business continuity plans are doing so now. These plans are not simply IT disaster recovery plans. In the case of Year 2000 technology failures, restarting the systems will not

fix the problem — they *are* the problem. Companies are looking at the weak points and potentially single points of failure in various business scenarios and developing contingency plans.

Impact on California From Around the Globe

California, the world's seventh largest economy, is very dependent on its imports and exports to the rest of the world. According to the International Trade Administration, California is this nation's leading exporter to Asia. Companies in California should be particularly vigilant about that area of the world. The most recent Gartner Group world status information indicates that companies in the Asian region have a 50% or greater chance of at least one mission-critical systems failure.

The exposure to risks coming from foreign countries may prompt governments to put restrictions on free trade. Retaliation, export barriers, and disruptions in the supply chain may have a worse effect on multinational enterprises, as well as those relying on foreign trade, than Year 2000 failures. For example, the food distribution industry is voicing concern about the readiness of infrastructures in some countries and is calling on governments for action. Enterprises operating in infrastructure sectors, such as energy, telecommunications, health care, and transportation, as well as enterprises with substantial trade with foreign countries, also are exposed to these risks. Enterprises should look at cases where supplies or access to markets may be jeop-

ardized by measures restricting free trade and at how competitors (especially market leaders) may try to exploit Year 2000 readiness information. They should use business intelligence to monitor the risk and tune their public relations and legal strategies for a timely response.

For this reason, California companies large and small need to understand the impact of a reduction in exports. Potentially, companies in all geographies will be adding a "cushion" to their inventory of key supplies during the latter half of 1999. This dependence on exports as a major source of revenue, as well as the complexity of the supply chain, should lead California companies to develop contingency plans.

Importance of Contingency Plans

Consider this scenario. It is July 1, 1999. An enterprise that manufactures large components as part of a major supply chain receives orders that must be delivered within six months. However, its order-processing system fails when calculating dates into 2000. The management team is called together to discuss what to do. It spends hours, perhaps even a day or more, discussing alternatives. As the organization's crisis team moves to address the issue, it is hampered by individuals who are not prepared for the necessary action. As days pass, the manufacturer's clients begin to execute their already-prepared contingency plans: find another supplier. When the manufacturer's contingency plans are finally ready to implement, its programming team comes up with a fix. The processing system is now ready.

"California companies large and small need to understand the impact of a reduction in exports....[D]ependence on exports as a major source of revenue, as well as the complexity of the supply chain, should lead California companies to develop contingency plans."

"In the U.S., industry segments such as health care, education, agriculture, construction, food processing, governments, and companies employing fewer than 500 people are lagging far behind in their compliance efforts. Many of them simply will not finish preparing critical systems by 2000."

For many clients, however, it is too late; they already have moved on. The manufacturer's business is damaged, perhaps irreparably.

A number of our clients have begun contingency planning; others have considered the issue. However, discussions with these clients reveal that the implications and considerations involved in preparing one's organization for potential Year 2000 failure are not always clearly understood.

It should be noted that it will not be possible for an organization to look at all its business processes. Therefore, companies should use a prioritization (or "triage") method to allocate resources where they are needed first: high-risk, mission-critical processes. These plans must be created by representatives of the business, working in concert with their Year 2000 program office.

Once the key processes for contingency planning are identified, a plan must be created,

with the following components:

- *A scenario, or description, that adequately describes when the plan must be executed.* This scenario should address both the severity and the potential duration of the failure.

- *Description of the steps to be taken.* For example, if a major technical asset fails, the contingency plan should not be simply: "Process manually." How will this be done? Who will perform the work? Where will these people be located?

- *Reference to previous work that must be completed in order for the contingency plan to be workable.* In the case of performing a process manually, workers must already have been identified (e.g., temporary workers from outside firms), and a location provided for their work. Otherwise, simply saying a process should be manually performed will not guarantee it will be.

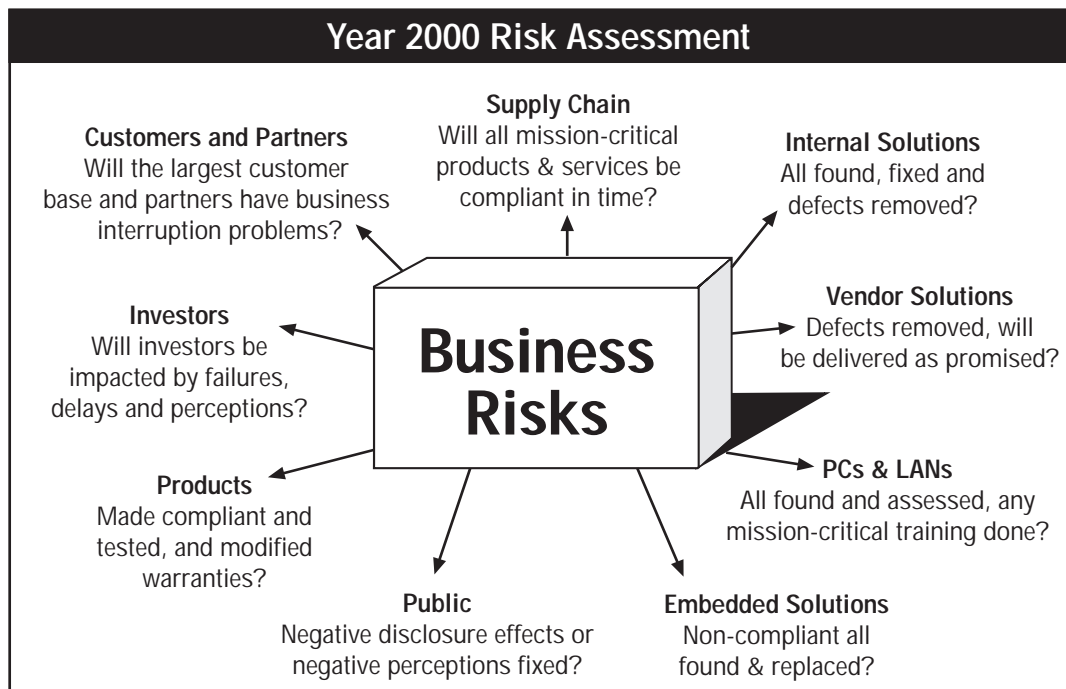
Summary

A great deal of progress has been made during the past year

in the U.S. and in several parts of the world. IT organizations in the U.S. have increased their spending for Year 2000 projects an average of six times over what was spent during 1997. Most U.S. companies now prioritize Year 2000 at the top, or number two (following Enterprise Resource Planning system projects, to replace legacy systems). Large companies in the U.S. have made the most significant progress; many of them will complete most of their compliance efforts by 2000. Even smaller companies in the U.S., in several industries, have made significant progress in the past year.

Despite this progress, there still are very serious risks for the U.S. and throughout the world. The gap between companies and governments furthest ahead and those furthest behind is widening even more since the laggards are moving much more slowly toward compliance. In the U.S., industry segments such as health care, education, agriculture, construction, food processing, governments, and companies employing fewer than 500 people are lagging far behind in their compliance efforts. Many of them simply will not finish preparing critical systems by 2000.

Interdependencies and interconnectivity between companies and across country borders are also extremely high in significance related to Year 2000 risks. Many of these interdependencies are not being addressed by either company, and many times their interconnections and data transfers cannot be easily tested. These are critically important in banking, government, health care, and for many global manufacturers.



Source: Gartner Group

Business Continuation Planning for Year 2000



By
Alan R. Arnold
Senior Manager,
Ernst & Young LLP

and

Michael Evans
Managing Partner,
E & Y Kenneth Leventhal

The largest industry analyst, the Gartner Group, expects the Y2K problem to be a \$300 billion to \$600 billion (U.S.) problem for the computer industry. Most people would assume this must be exaggerated by a few billion. Based on our experience so far, we don't think the Gartner number is going to be far off.

Recent surveys indicate that more than 50% of U.S. data processing organizations will not have their software Y2K ready by December 31, 1999. The percentage is even higher for data processing organizations outside the U.S. In Europe, the scarce technical and monetary resources needed to fix the Y2K problem also must be used to modify information systems to handle the adoption of a common currency.

Y2K Assessments for Small Business

Some small businesses don't expect to have Y2K problems because their systems are much newer than older legacy mainframe systems. Mainframes will have more problems, but midrange systems must be checked for Y2K readiness as well. Unfortunately, many of the same coding techniques used on mainframe systems also were used in midrange development environments. One thing is sure: A company will not know what shape its source code is in until an assessment is done. It cannot bet its business on a hunch that the source code is Y2K ready.

Application software is probably one of the most critical areas to address. A common problem is that many businesses do not purchase source code for programs. Does the business own the source code? For companies that have it, does the source match the objects that are currently running its production environment?

If a company has the source code, the two leading techniques for addressing the Y2K issue are referred to as "expansion" and "procedural." With the expansion technique, the database is actually modified to capture century information. The procedural technique intercepts the bad date, converts it to a good date for the program, and then passes on the correct parameters. Which technique is better? It depends on the situation. We favor the expansion technique when disk space is available because it is a true fix to the problem, and functions such as query and index key sorts based on date fields will continue to work properly.

If a business does not have

the source code, it is in trouble. There is no silver-bullet solution. It will have to start looking for alternatives such as upgrading, changing, or retiring its applications. These options take a lot of time and money to work through. If the only option is to implement a new software solution, time is needed to review, select, and implement a package.

Managing the project source codes is just one of the issues that has to be addressed when a company begins its journey to Y2K readiness. Good project management is the key to successfully dealing with these issues. Project management includes overseeing all phases of the Y2K project, that is, dealing with the central and peripheral issues that must be addressed for the company to become Y2K ready.

It is necessary to ensure that someone in the organization is reviewing *everything*. Everything should be assumed non-ready until proven otherwise. All of these issues should be logged and documented by the project manager. A master schedule containing all the IT issues as well as the non-IT issues needs to be created. Coordinating and implementing the fixes must be done in a manner that minimizes business disruption. Y2K work needs to be prioritized by the potential effect the problem will have on the business. All problems that will stop the business must be given the highest priority. Potential risk factors must be understood and detailed contingency plans put in place.

Above all, good communication is necessary to best prepare a business for the Year 2000. Problems and the potential impact must be understood at the highest levels of management.

"Recent surveys indicate that more than 50% of U.S. data processing organizations will not have their software Y2K ready by December 31, 1999. The percentage is even higher for data processing organizations outside the U.S."

"Fixing the financial reporting software for Y2K is of little benefit if on December 31 the production line shuts down, the lights go out, or the heating system shuts off. The Y2K issue as it relates to facilities and production may be the most significant risk to a business today."

We anticipate there will be many lawsuits due to Y2K problems. To avoid these, companies should start an assessment today by getting a good inventory of problems and potential problems. A conversion strategy should be selected, then implemented in a controlled fashion that does not disrupt the company's business. With any luck, the impact will be minimal.

Technical vs. Business Problem

From a technical perspective, the Y2K problem is not complex. Some dates will not process correctly when used in arithmetic calculations, date comparisons, and sequencing (sorts). From the business perspective, these technical problems escalate into larger issues such as orders that will not bill correctly, supply channels that will be botched up, accounting reports that will not age correctly, and invoice systems that will not bill correctly.

A company that does not understand the magnitude of its Y2K problem may be vulnerable to serious damage or, even worse, complete failure. Failure of a business may be construed as an extremist opinion but the problem is real. Unfortunately, far too many companies are still ignoring it.

Planning can be the most difficult — and sometimes most overwhelming — part of a company's Year 2000 preparations. Many companies simply do not know where to start. For others, each time they feel they have a handle on it, another hidden issue appears. Application issues are usually at the center of Y2K projects, but there are other factors that must be considered. For instance, many other systems —

such as PCs, BIOS-controlled systems, bar code readers, measurement and weight systems, UPS systems, laser printers, climate control systems, and security systems — may have problems as well.

The Y2K problem is not difficult to solve once a business has put together a detailed project plan. Of course, that plan needs to be supported by an appropriate budget and technical resources. The amount of time or money needed should not be underestimated. This is one of the first mistakes made on Y2K projects.

Unfortunately, in many cases, making applications Y2K ready will not result in a company being better or more competitive than it is today. On the other hand, choosing to ignore the problem could result in the company going out of business. For this reason, many companies are looking at replacement applications that offer increased functionality in addition to fixing the Y2K problem. This is a good option for businesses that have enough time, but time is the one thing typically lacking in a Y2K project.

The replacement option is being eliminated quickly for some companies because they won't have enough time, but this option needs to be well thought out and understood. It should not be assumed that fixing old applications will be easier, faster, and less expensive. For example, if a business doesn't own the source code or is missing large amounts of it, the problem will be extremely difficult to fix.

What Else Can Go Wrong?

Frequently overlooked are production and operation facilities. Machinery, building systems such as HVAC, lighting, el-

evators, and most production machinery are all controlled by a computer. Fixing the financial reporting software for Y2K is of little benefit if on December 31 the production line shuts down, the lights go out, or the heating system shuts off. The Y2K issue as it relates to facilities and production may be the most significant risk to a business today. Companies should make sure facilities they utilize are Y2K compliant in the following areas: 1) continuity of outside services including utilities, electricity, gas, fuel, oil, water, communications, and sewage; 2) environmental and refrigeration systems availability (internal); 3) integration of security and life-safety systems; and 4) mission-critical systems. Generally, these systems will fall into two categories: equipment that operates using firmware and software embedded within the microprocessors; and equipment remotely controlled by separate microprocessors.

Our estimate is that up to 20% of these systems will fail if not fixed. The critical and costly part is identifying the 20% and fixing those most at risk. Thus, since every business uses real estate or has equipment, every business will be affected by Y2K.

Conclusion

Extremist Y2K examples should not scare companies into ignoring Year 2000 issues. There are real Y2K problems happening in the industry today, and many more appear as we approach the New Millennium. Not only do businesses need to fix their own Y2K problems, they must be aware of their vulnerability to other companies' problems. Everyone will be affected one way or another. Be prepared.

Local Governments Plan for Year 2000



By Steven A. Steinbrecher

*Chief Information Officer,
Contra Costa County*

It is now January of 1999. Do you know where your Year 2000 project is? If not, you should. The major issue local governments face with the Year 2000 issue, Y2K, or millennium bug, as it is called, is that we *really* don't know what is going to happen when the clock strikes 0000 on January 1, 2000. In the absence of *really* knowing, we believe it is best to be prepared for a realistic series of events, especially given the other alternatives of "The Sky is Falling" (Chicken Little), or "Nothing is Going to Happen at All" (complete denial) scenarios.

Let's face it. If you are a public official and your jurisdiction has not had an internal awareness campaign and at least assessed the impact of the Y2K problem on your computer systems and embedded chip technology (that's all those things like electronic door locks, gas pumps, traffic signals, burglar

alarms, heating and air conditioning units, elevators, police cars, etc.), you might consider updating your resume and passport this year.

Even if you have been working hard on this project for a couple of years now, there should still be some uncertainty in wondering whether you are covering all the right bases. After all, just given the potential number of embedded chips located in the State of California (something in the tens of millions), there should be cause for concern.

Taking a Proactive and Positive Approach

It is the belief of those of us working on the problem in Contra Costa County that we need to approach this issue with a "Proactive and Positive Attitude." While there is no one "right" way to address this issue, Contra Costa County's approach has focused on the following issues:

- Internal Data Center remediation efforts — This involves all the centralized computing applications and operations.
- Wide Area Network (WAN) infrastructure — This is the telecommunications backbone throughout the County, which includes phone lines, routers, hubs, switches, etc., and external interfaces with other agencies.
- Our fleet of desktop computers and the Local Area Networks (LANs) in our 35 county departments.
- The embedded chips throughout the County's numerous buildings, cars, the airport, and mechanical equipment.
- Legal due diligence, coordinated business resumption planning, potential disaster

and event planning, and community awareness.

Contra Costa County is using the following methodology to achieve its goals in a proactive and positive manner:

Executive Involvement

Executive sponsorship and involvement is *crucial* for the success of a project such as this. Contra Costa County's department heads, the Board of Supervisors, and the County Administrator have been receiving regular briefings from the County's Chief Information Officer since April 1996. If the Y2K Project Manager in your county is not communicating with executive management on a regular basis, she or he needs to.

Departmental Planning

Individual county departmental computer systems, applications, and local area networks are the responsibility of individual county departments. To assist in this effort, monthly meetings are held between departmental staff and the County's Year 2000 Coordinator. In addition, the County has developed a Web site loaded with business and technical reference information. Management is provided with ongoing education regarding the necessity for early Year 2000 compliance at the departmental level.

Comprehensive Remediation Program

In early 1998, the County initiated a comprehensive Year 2000 Remediation Program for all affected components. This program includes Year 2000 business recovery education, embedded chips, emergency recovery procedures, risk and asset management, legal "due diligence," and Office of Emer-

"Even if you have been working hard on this project for a couple of years now, there should still be some uncertainty in wondering whether you are covering all the right bases. After all, just given the potential number of embedded chips located in the State of California...there should be cause for concern."

"It would appear prudent for each county organization to anticipate failure of one or more of its systems and to have a plan in place to respond."

agency Services and disaster planning for calendar year 1999. The County has completed an inventory of assets (both IT and non-IT), ranked in the following categories:

- 1) Necessary for life, health, welfare, and safety of citizens
- 2) Would cause monetary loss to the County
- 3) Application systems with direct public interface
- 4) Systems that could be inoperable for up to two weeks with no adverse impact

The County has been working toward the Y2K remediation of these assets in order of importance.

Disaster Recovery Test

Coordination between all players is essential. It is anticipated the County will hold a coordinated, countywide "non-fatal" Year 2000 disaster recovery test during 1999. The disaster recovery drill will concentrate on assets in the first three

categories listed above; it is in the planning stages at this time. The present plan is for the County Office of Emergency Services to coordinate this test, with assistance from multiple departments. The County is hopeful the State will work with it, or multiple counties and cities, in a similar exercise.

Embedded Chip Remediation

Embedded chip (non-IT) remediation is in the inventory, risk assessment, and remediation stages, with most of the effort being managed by the County's Department of General Services. It is focusing on the Sheriff's Office, Health Services Division, Fire Department, and Public Works. To facilitate this process, the County has access to two databases, one state and one national, to obtain information regarding the literally thousands of embedded chip devices. It appears that this may be the most vulnerable area of exposure, based on the sheer number of embedded mi-

crochip devices in operation, their physical location, the lack of documentation by the manufacturer(s), and the length of time many of these devices have been in service.

It would appear prudent for each county organization to anticipate failure of one or more of its systems and to have a plan in place to respond. The key to Contra Costa County's Year 2000 resolution efforts has always been to concentrate on those functions considered life threatening or security related for citizens, and those functions that would disrupt the County's revenue generation and collection processes.

Public Awareness Campaign

Finally, Contra Costa County has been involved in a public awareness campaign, which it hopes to gear up during 1999. In addition to internal executive and senior management, the County's Chief Information Officer has worked with local city staff, risk managers, regional emergency services managers, and the news media to discuss the various facets of Year 2000 activities, how we are dealing with them, planning activities, and the need for coordinated efforts. It is hoped that by approaching these issues in a proactive and positive manner, citizens will understand that while there is some expectation of potential problems, local government is taking a realistic and logical approach in dealing with the Year 2000 issue.

California Local Government Year 2000 Compliance Survey Results¹

Target Groups	Survey Population	Total Respondents	
Cities	466	308 (66%)	
Counties	58	48 (83%)	
Special districts ²	150	46 (31%) ³	
		Yes	No
Y2K compliance plan in place?		73.6%	26.4%
Designated managers for compliance plan?		87.8%	12.2%
Designated Y2K compliance budget?		58.1%	41.9%
Expect Y2K compliance by end of 3rd quarter, 1999?		82%	18%

¹ Survey was conducted in the summer of 1998 by the CA Assn. of Local and State CIOs.

² Representative sampling of 5,000 special districts in California

³ Only 46 of 150 districts targeted for sampling were interviewed due to difficulties getting accurate information on contacts, location, and time constraints.

Source: Dept. of Information Technology *October 1998 Quarterly Report*

Survey of Year 2000 Liability Legislation



By Daniel Cooperman
*Senior Vice President,
General Counsel & Secretary,
Oracle Corporation*

The Year 2000 problem has increasingly been garnering serious attention in the press as we approach the Millennium. The problem has inspired many frightening predictions of catastrophic litigation. Some have estimated that litigation costs will approach \$1 trillion worldwide. While litigation of that scope would clearly impact California's economy, whether it comes to pass is far from certain. Nonetheless, as if to embrace these dire predictions of runaway litigation, the federal government and many states, including California, have already enacted and are considering legislation to address the Year 2000 issue.

While some Year 2000-related bills have addressed specific topics such as tax credits for Year 2000 spending and re-deployment of state resources to address Year 2000 problems, legislative initiatives addressing liability have thus far fallen into three general categories: laws limiting private parties' liabil-

ity for Year 2000 computer failures; laws immunizing states from Year 2000 liability; and laws governing Year 2000 information disclosures. This paper summarizes legislative efforts to date to enact these three types of legislation at both the state and federal level and offers the author's perspective on these initiatives.

Legislation Immunizing Government Entities

At least 17 states, including California, have considered or passed laws immunizing government entities from liability. The proposed California statute, SB 2000, died last session in the Senate Judiciary Committee. Immunity legislation has been enacted in Nevada, Florida, Hawaii, Virginia, and Georgia; passage of similar laws in other states appears likely. However, the federal government has not considered such legislation.

Typical of these statutes is the law recently passed in Florida, which provides: "There shall be no cause of action at law against the state, its agencies or instrumentalities, or any unit of local government for actions or inactions that are attributable to a year 2000 computer date calculation failure, and there shall be no waiver of sovereign immunity with respect to the same."

Nevada's statute is also simple and, in fact, appears to sweep more broadly, as it provides for immunity from suits based on a state computer system that "produced, calculated or generated an incorrect date, regardless of the cause of the error." A computer program could calculate or generate "an incorrect date" without having a Year 2000 problem.

These laws may not have a significant impact, as many

states generally are already immune from liability except in limited circumstances. In addition, these laws may not inspire public confidence in state efforts to address the problem. Florida's statute self-servingly proclaims that "[t]he Legislature finds that the state and units of local government have taken due care to prepare for the date change that will accompany the Year 2000" — a claim that may well be tested come the new Millennium.

Legislation Governing Year 2000 Information Disclosures

California and Congress have each passed laws protecting companies for disclosures regarding Year 2000 compliance efforts. The laws are intended to stimulate the free flow of information among companies and thereby encourage more effective remediation efforts. The recently enacted federal Year 2000 Information Readiness and Disclosure Act ("IRDA") provides that a written Year 2000 disclosure, if properly labeled, cannot be used as evidence in a lawsuit against the discloser. The law also provides that a false statement regarding Year 2000 compliance cannot form the basis of a lawsuit against the maker unless the plaintiff can show that the statement was knowingly false or was made with reckless disregard for the truth. The law also contains complex grandfathering provisions, whereby a company can obtain protection for statements made prior to the law's enactment.

The California statute is much simpler. It provides that any person that discloses Year 2000 information "shall not be liable for damages in any tort action" caused by "the use of the information disclosed." Again,

"The [Y2K] problem has inspired many frightening predictions of catastrophic litigation. Some have estimated that litigation costs will approach \$1 trillion worldwide. While litigation of that scope would clearly impact California's economy, whether it comes to pass is far from certain."

"...[T]he threat of litigation has undoubtedly (and properly) been a motivating factor for companies seeking to achieve Year 2000 compliance for new products and to address customer concerns over non-compliant products; limiting liability may deter some from taking reasonable steps to achieve compliance."

the law excludes protection for statements that are knowingly false or that were made with reckless disregard for the truth. However, California's law may be preempted by the IRDA.

While these laws are well meaning, they contain enough loopholes and uncertainties that it is questionable whether they will actually spur more complete disclosures. Under the IRDA, for example, a plaintiff relying on a Year 2000 statement will simply allege fraud and recklessness, and thereby likely prevent a quick resolution to the case.

Legislation Limiting Year 2000 Liability

Liability-limiting provisions have created the most controversy. At least seven states have considered such bills; California has considered two, both of which died last session in the Assembly Judiciary Committee. California is among the most active states in the country in considering such provisions, perhaps not coincidentally because of the state's well-developed high tech industry. Liability-limiting legislation has not passed in any state but may be headed for passage in Florida.

These statutes present a wide range of features, highlighted by the two failed California bills, AB 1710 and AB 1934.

AB 1710 generally exempted computer hardware and software vendors from Year 2000 claims based in tort as long as the defendant could show that it provided notice of any Year 2000 defect and offered a free upgrade to fix the problem. Companies sued for losses stemming from defective hardware or software purchased from another vendor

would also have been immune from suit. The bill excluded claims for personal injury and also allowed plaintiffs to pursue contract-based claims. AB 1934 was much simpler: it simply established a cap of \$250,000 for non-economic losses in Year 2000 cases.

Other states have considered various approaches. Florida's proposed bill is particularly complex. Among other things, the bill imposes an express warranty for Year 2000 solution providers that would override existing contract rights, requires solution providers to maintain certain levels of liability insurance, overrides existing contract provisions limiting liability, severely limits the availability of the class action as a litigation device, and provides for attorney's fees for prevailing parties in Year 2000 litigation.

In contrast, Texas considered a bill that simply provided that Year 2000 plaintiffs could only recover losses for personal injury, wrongful death, and costs to repair defective software or hardware. Similarly, a Pennsylvania bill would have limited plaintiffs to "direct" damages, defined as personal injury, property damage, and costs to repair defective software or hardware. However, that bill would not have applied to claims based on fraud, intentional harm, gross negligence, or contract terms.

Finally, an Illinois bill would have immunized banks from claims by parties "not in privity of contract," but did not address other industry segments.

In addition, Congress has considered a number of different proposals that would limit liability, including a complex and comprehensive bill proposed by

Rep. David Dreier of California.

While these bills are well intentioned, legislators should be cautious. Companies doing business nationwide could be confronted with a myriad of differing and potentially inconsistent liability standards unless the issue is addressed at the federal level. Moreover, in many cases, existing contracts already address parties' respective rights and remedies in this area, and legislators should be cautious of altering those parties' settled expectations. In addition, the threat of litigation has undoubtedly (and properly) been a motivating factor for companies seeking to achieve Year 2000 compliance for new products and to address customer concerns over non-compliant products; limiting liability may deter some from taking reasonable steps to achieve compliance. Finally, new legislation may breed litigation over the meaning and scope of the law. Changing the law also creates further uncertainty for corporate managers over Year 2000 issues.

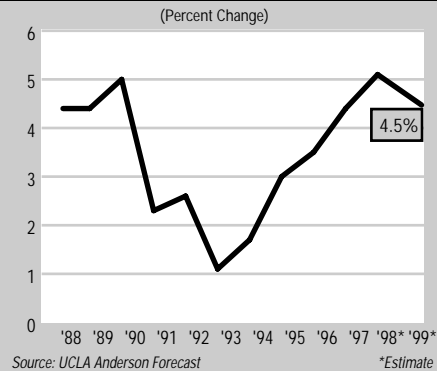
Conclusion

Most legislators who back Year 2000 liability legislation cite the high cost of potential litigation as a major justification. The current climate of extreme anxiety has led to strong rhetoric in support of such laws. Clearly, California's businesses and economy would be severely hampered even if the dire litigation predictions are only half true. Nonetheless, before enacting Year 2000 liability-limiting legislation, legislators must thoughtfully consider the broad potential ramifications of such new statutory measures.

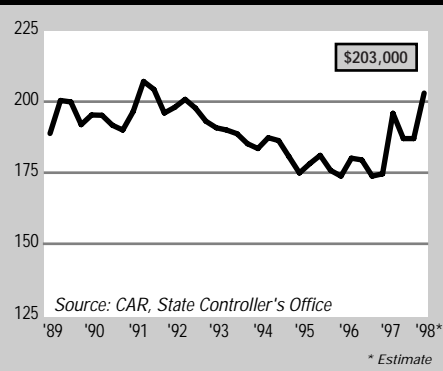
Facts and Figures

Important Information About California

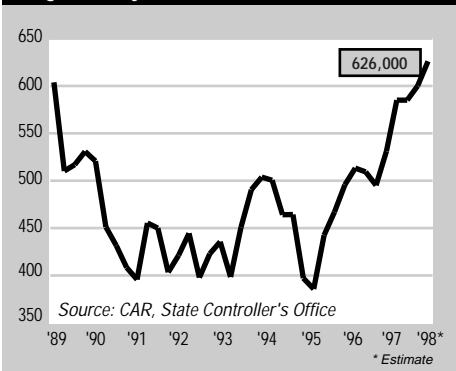
Growth of Average Wage, CA



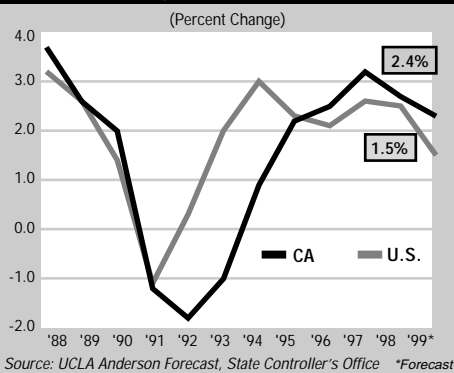
Median Home Price (In Thousands)



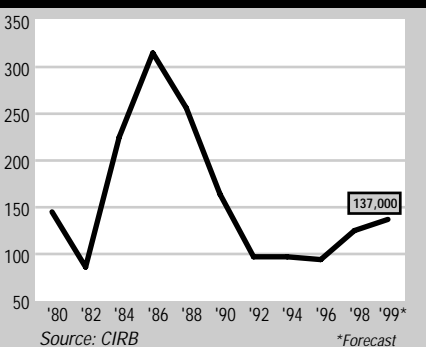
Single Family Home Sales (In Thousands)



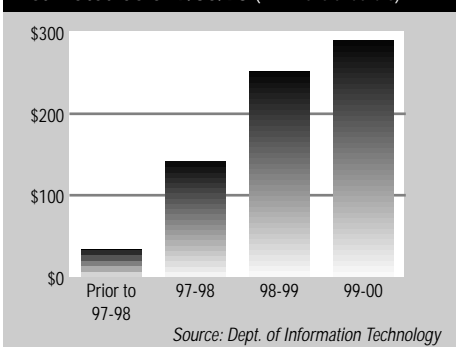
Non-farm Employment Growth, CA vs U.S.



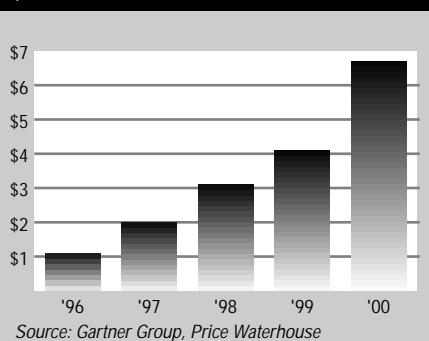
Residential Building Permits (Thousands of Units)



Cumulative CA Y2K Remediation Costs Estimated as of 9/30/98 (in millions of dollars)



Growing Cost of Y2K Compliance (per line of code corrected)



Y2K vs. Other Events (in billions of dollars)

WWII	\$ 4,200
Y2K	\$ 600
Vietnam War	\$ 500
Kobe Earthquake	\$ 100
LA Earthquake	\$ 60

Source: Gartner Group, Congressional Research Service

10 U.S. Industries Most Vulnerable to Y2K Business Disruption (based on 50-industry survey)

Financial Services
Insurance
Other Transport
Industrial Machinery
Communication Services
Instruments
Business Services
Utilities
Wholesale Trade
Auto Repair/Rental

Source: WEFA

In Upcoming Editions of the Controller's Quarterly:

Economic
Forecast '99



Venture Capital
and California's
Growth



The Global
Economy



Regional
Economic Profiles



Budgeting
for the Future



Small Business in
California's
Economy



Kathleen Connell
California State Controller
P.O. Box 942850
Sacramento, CA 94250
(916) 445-2636

<http://www.sco.ca.gov>